

WHAT IS CLAIMED IS:

1 1. A method for securing alterable data in a remotely managed system comprising
2 the steps of:

3 providing protected storage accessible only by Basic Input Output System (BIOS)
4 code;

5 storing a symmetrical encryption Key in said protected storage;
6 encrypting normally unaccessible (NA) data with said symmetrical encryption
7 Key; and

8 storing said NA data and accessible non-encrypted (ANE) data in an unprotected
9 electronically erasable programmable read only memory (EEPROM) with existing write
10 protect algorithms.

1 2. The method of claim 1 further comprising the steps of:

2 altering said ANE data by issuing an existing write request to said BIOS from
3 said write protect algorithms for said EEPROM; and

4 updating said ANE data in said EEPROM.

1 3. The method of claim 1 further comprising the steps of:

2 accessing said NA data via a change request issued to said BIOS over a secure
3 communication link;

4 validating said change request;

5 retrieving said symmetrical encryption Key by said BIOS in response to said
6 validated change request;

7 using said symmetrical encryption Key to decrypt and alter said NA data;

8 encrypting said altered NA data using said symmetrical encryption Key; and

9 storing said altered encrypted NA data in said EEPROM.

1 4. The method of claim 1 further comprising the steps of:

2 hashing said ANE data and encrypting said Hash with said symmetrical
3 encryption Key;

4 storing said encrypted Hash with said ANE data;

5 computing a Hash of configuration data in said ANE data on a boot-up request;

6 decrypting said stored encrypted Hash of said configuration data;

7 comparing said decrypted Hash of said stored configuration data to said computed

8 Hash of said configuration data from said ANE data;

9 booting normally in response to a compare of said decrypted Hash and said
10 computed hash; and

11 issuing tamper notification and initiating recovery processes on a non-compare
12 of said decrypted Hash and said computed hash.

1 5. A computer program product for securing alterable data in a remotely managed
2 system with minimal secure storage, said computer program product embodied in a
3 machine readable medium, including programming for a processor, said computer
4 program comprising a program of instructions for performing the program steps of:

5 providing protected storage accessible only by Basic Input Output System (BIOS)
6 code;

7 storing a symmetrical encryption Key in said protected storage;
8 encrypting normally unaccessible (NA) data with said symmetrical encryption
9 Key; and

10 storing said NA data and accessible non-encrypted (ANE) data in an unprotected
11 electronically erasable programmable read only memory (EEPROM) with existing write
12 protect algorithms.

1 6. The computer program product of claim 5 further comprising the program steps
2 of:

3 altering said ANE data by issuing an existing write request to said BIOS from
4 said write protect algorithms for said EEPROM; and

5 updating said ANE data in said EEPROM.

1 7. The computer program product of claim 5 further comprising the program steps
2 of:

3 accessing said NA data via a change request issued to said BIOS over a secure
4 communication link;

5 validating said change request;

6 retrieving said symmetrical encryption Key by said BIOS in response to said
7 validated change request;

8 using said symmetrical encryption Key to decrypt and alter said NA data;
9 encrypting said altered NA data using said symmetrical encryption Key; and
10 storing said altered encrypted NA data in said EEPROM.

1 8. The computer program product of claim 5 further comprising the program steps
2 of:

3 hashing said ANE data and encrypting said Hash with said symmetrical
4 encryption Key ;

5 storing said encrypted Hash with said ANE data;

6 computing a Hash of configuration data in said ANE data on a boot-up request;

7 decrypting said stored encrypted Hash of said configuration data;

8 comparing said decrypted Hash of said stored configuration data to said computed
9 Hash of said configuration data from said ANE data;

10 booting normally in response to a compare of said decrypted Hash and said
11 computed hash; and

12 issuing tamper notification and initiating recovery processes on a non-compare
13 of said decrypted Hash and said computed hash.

- 1 9. A computer system comprising:
2 a central processing unit (CPU);
3 a random access memory (RAM);
4 an electronically erasable programmable read only memory (EEPROM);
5 an I/O adapter; and
6 a bus system coupling said CPU to said EEPROM, said I/O adapter, and said
7 RAM, wherein said CPU further comprises:
8 protected storage accessible only by Basic Input Output System (BIOS) code;
9 circuitry for storing said symmetrical encryption Key in a protected storage;
10 circuitry for encrypting normally inaccessible (NA) data with said symmetrical
11 encryption key; and
12 circuitry for storing said NA data and accessible non-encrypted (ANE) data in a
13 non-protected electronically erasable programmable read only memory (EEPROM) with
14 existing write protect algorithms.
- 1 10. The data processing system of claim 9 further comprising:
2 circuitry for altering said ANE data by issuing an existing write request to said
3 BIOS from said write protect algorithms for said EEPROM; and
4 circuitry for updating said ANE data in said EEPROM.
- 1 11. The data processing system of claim 9 further comprising:
2 circuitry for accessing said NA data via a change request issued to said BIOS over
3 a secure communication link;
4 circuitry for validating said change request;
5 circuitry for retrieving said symmetrical encryption Key by said BIOS in response
6 to said validated change request;

7 circuitry for decrypting and altering said NA data said using said symmetrical
8 encryption Key;
9 circuitry for encrypting said altered NA data using said symmetrical encryption
10 Key; and
11 circuitry for storing said altered encrypted NA data in said EEPROM.

1 12. The data processing system of claim 9 further comprising:
2 circuitry for hashing said ANE data and encrypting said Hash with said
3 symmetrical encryption Key;
4 circuitry for storing said encrypted Hash with said ANE data;
5 circuitry for computing a Hash of configuration data in said ANE data on a
6 boot-up request;
7 circuitry for decrypting said stored encrypted Hash of said configuration data;
8 circuitry for comparing said decrypted Hash of said stored configuration data to
9 said computed Hash of said configuration data from said ANE data;
10 circuitry for booting normally in response to a compare of said decrypted Hash
11 and said computed hash; and
12 circuitry for issuing tamper notification and initiating recovery processes on a
13 non-compare of said decrypted Hash and said computed hash.